Trust Frameworks in Digital Identity

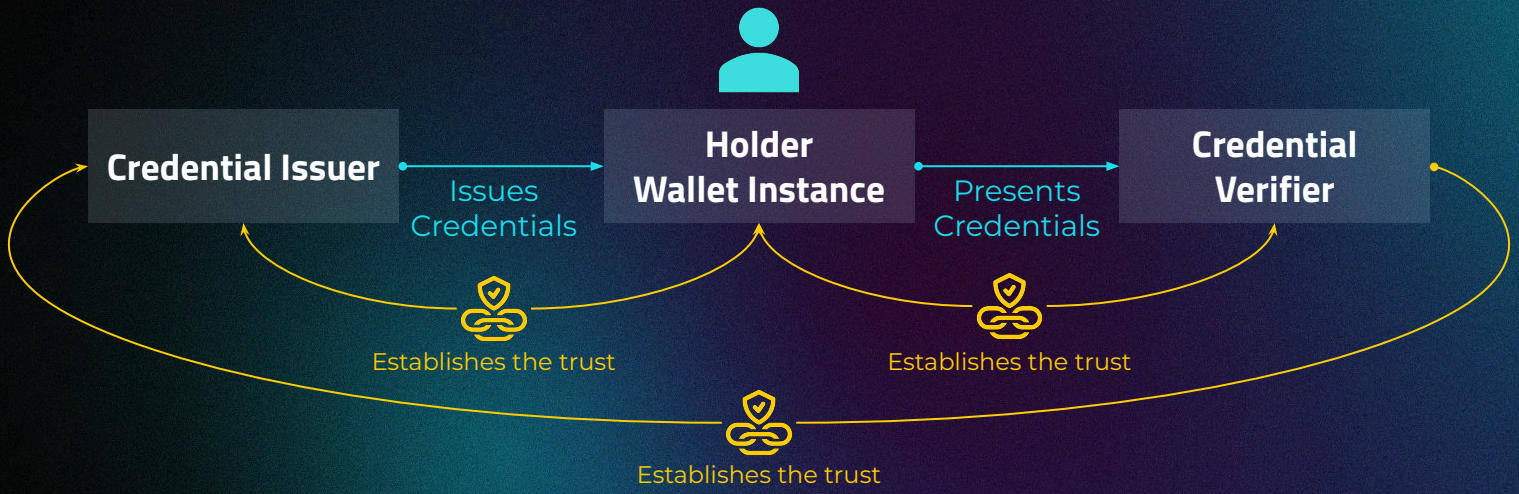
Building Bridges Between EUDIW and OpenID Federation

3rd International Workshop on Trends in Digital Identity (TDI 2025)
03.02.2025 - Bologna - Italy

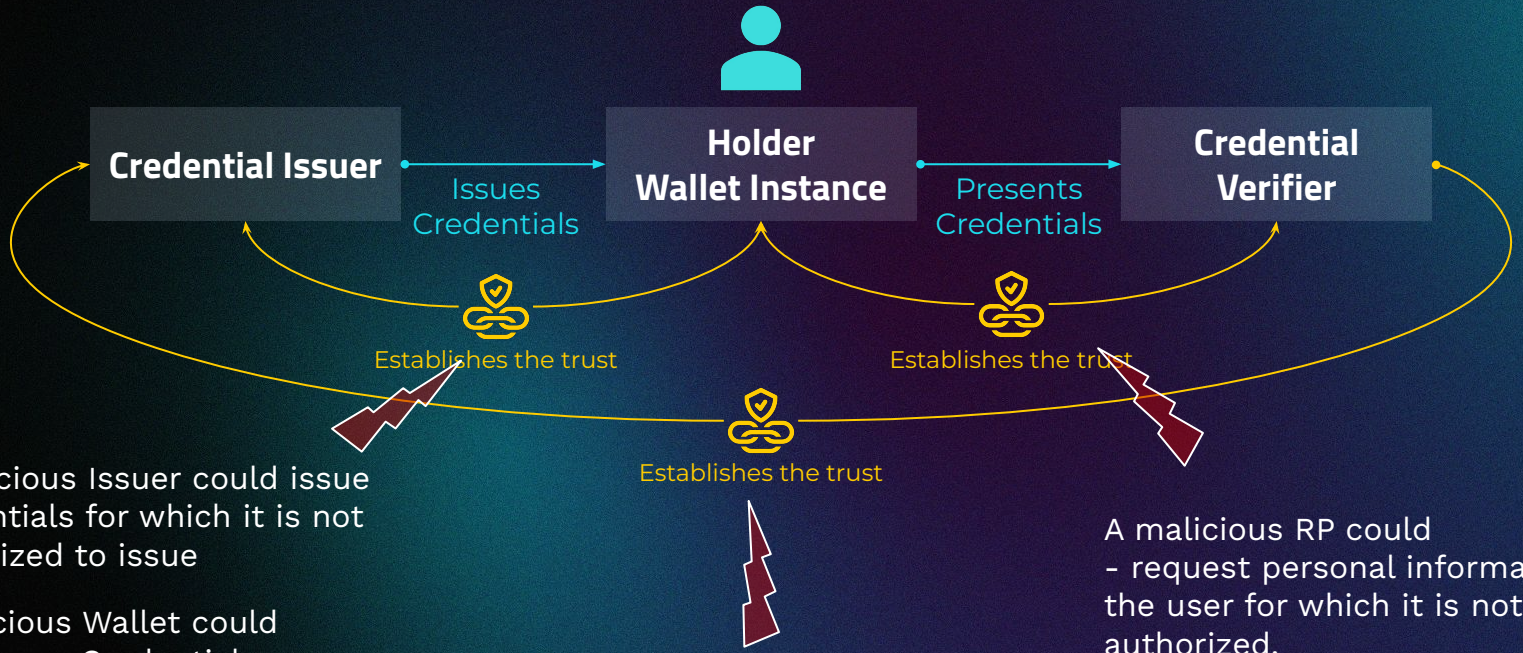
SPEAKERS: FRANCESCO ANTONIO MARINO / PASQUALE CERQUA

POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO

What exactly is meant by “TRUST”?



1. Trustworthiness and reliability of Credential Issuers, Verifiers and Wallet Providers (as legal entities) and the technical components provided by them (e.g., Wallet app).
2. Authenticity and integrity of Credentials and digital artefacts during Issuance and Presentation.



A malicious Issuer could issue Credentials for which it is not authorized to issue

A malicious Wallet could obtain user Credentials

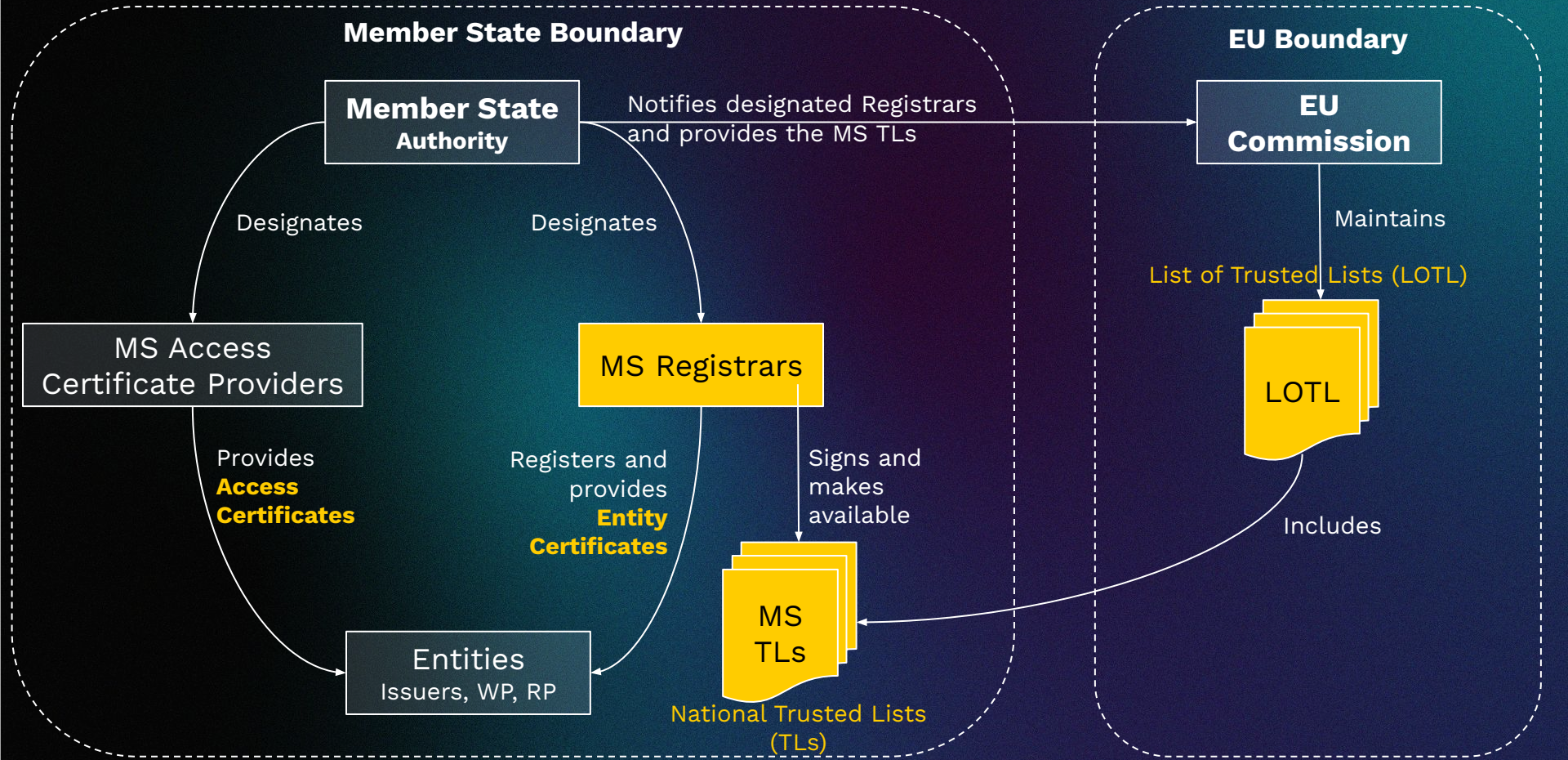
An RP would not know which Issuer is eligible for issuing determined Credentials.

A malicious RP could
- request personal information from the user for which it is not authorized.
- send a request requiring the response to be submitted to a URI on a domain outside the RP

How to solve this?

1. **Cryptographic keys** exclusively assigned to and used by their owner
2. **Digital certificates** accessible to third parties for trust verification

How is Trust being addressed in EUDIW?

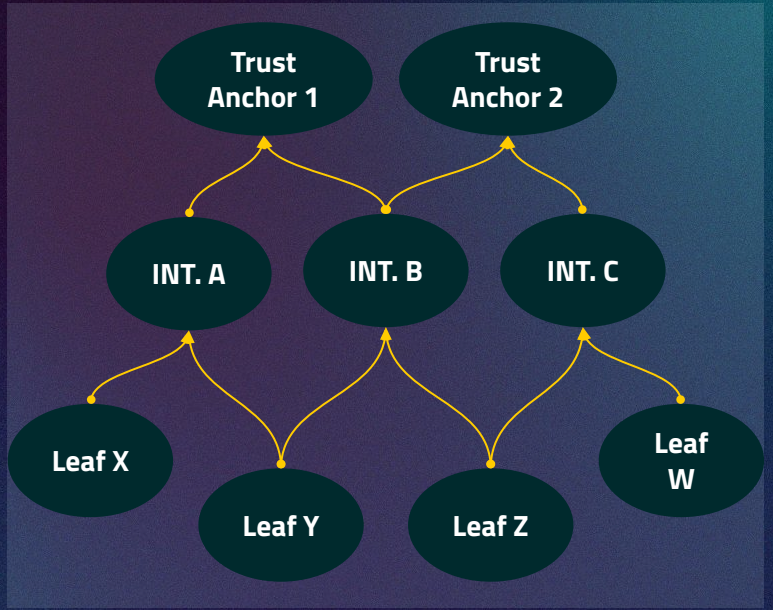

Member State Boundary
EU Boundary
Member State Authority
Notifies designated Registrars and provides the MS TLs
EU Commission
Designates
Designates
Maintains
List of Trusted Lists (LOTL)
MS Access Certificate Providers
MS Registrars
LOTL
Provides Access Certificates
Registers and provides Entity Certificates
Signs and makes available
Includes
MS TLs
Entities
Issuers, WP, RP
National Trusted Lists (TLs)

Trust Frameworks in Digital Identity

OpenID Federation: a different view on Trust

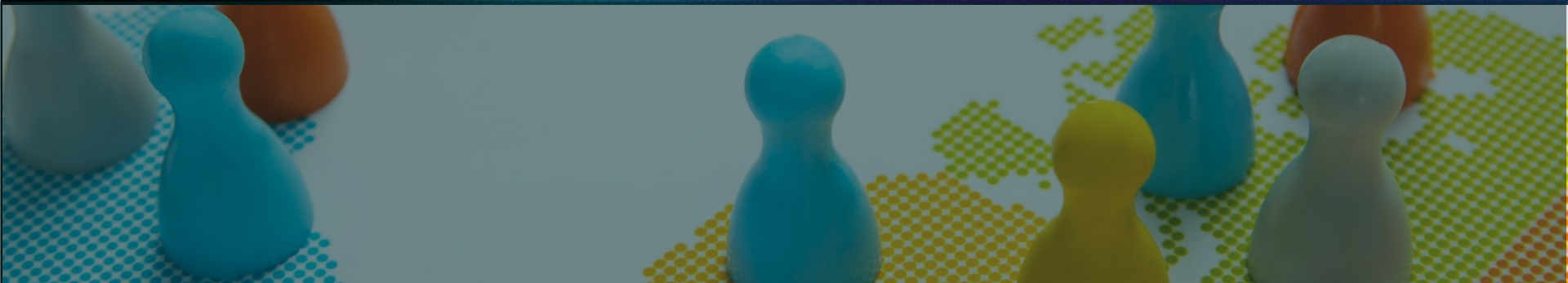
Hierarchical tree structure

- Trust Anchors (root of trust) publish digital certificates relating to intermediary or leaves
- Intermediaries publish digital certificates relating to leaves
- Leaves publish Entity Configurations (self signed JSON document) with their configuration and protocol related data (Metadata)
- Digital certificates (Subordinate Statement) and protocol related data are publicly available through Federation APIs
- Automatic Registration and trust evaluation using Federation APIs



	EU Trusted List	OpenID Federation
Formats	**Trusted Lists**: XML according to ETSI TS 119612 Cryptographic keys: **X.509 Certificates** published in 1988 (before the WWW in 1989, HTTP in 1991, Web APIs, JSON in 2001 and JWT in 2010)	**Verifiable Statements**: Signed JSON format (JWT) including Metadata and cryptographic keys in JWK Set Format: - Raw parameters - **X.509 certificates** (by value or by reference)
Update and Distribution Mechanisms	Member States publish **Trusted Lists** (TL). The European Commission publishes a **List of Trusted Lists** (LOTL), which includes all national TLs. The Commission provides a public tool to access both national TLs and the LOTL. ➔ **Static** trust management ➔ **Manual** updates and distribution	Publication of Subordinate Statements through a **WEB API interface**. ➔ **Dynamic** trust management ➔ **Automatic** updates and distribution

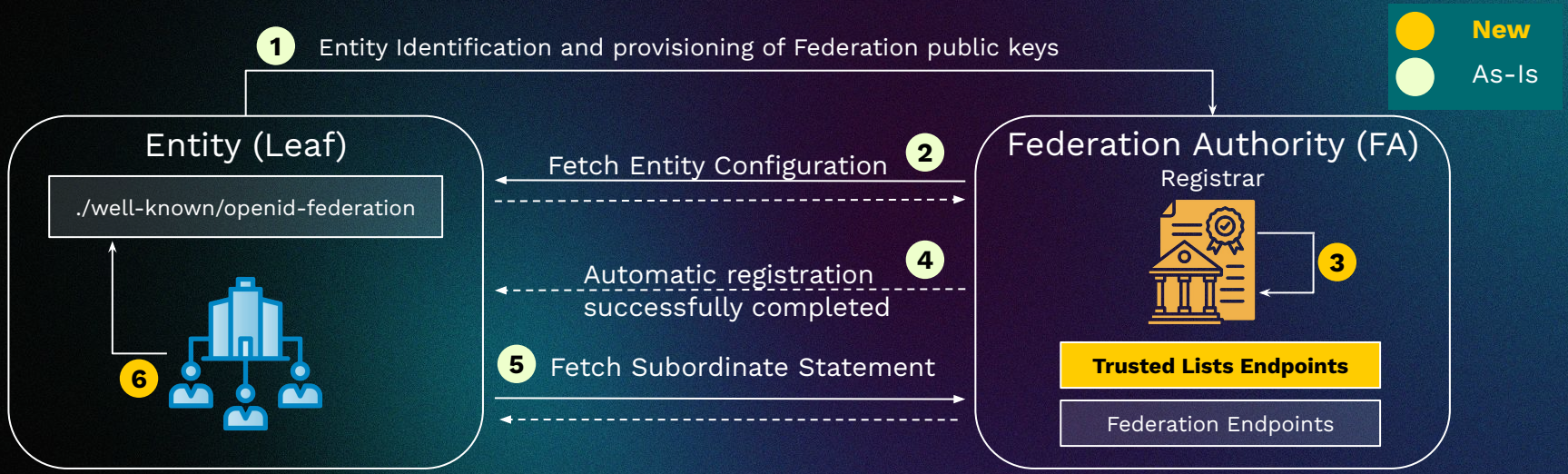
How to use OpenID Federation in the EUDIW context?




Problem Statement
The distribution of the Digital Certificates
during the Registration Phase
Possible Approach:
Through the Subordinates Statements

Before Registration

➔ **Generate Trusted Lists** including **X.509 Registrar Certificate** making them **publicly available through new federation endpoints**



3

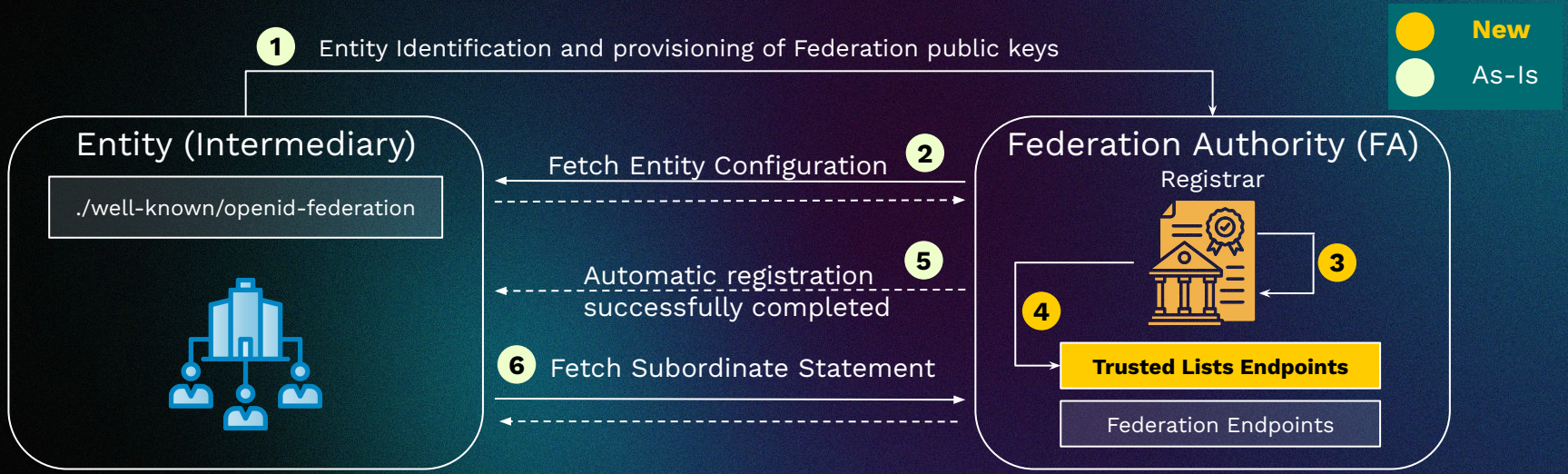
➔ Validate Entity Configuration (check that it is signed with private key related to the Federation public key)
➔ **Generate X.509 Certificate** attesting Federation public keys and **signed with X.509 Registrar Certificate** (FA-CERT)
➔ Generate Subordinate Statement **including X.509 Federation Certificate** (SUB-CERT) **in JWK Object (x5c parameter)**

6

➔ **Generate a X.509 Access Certificate** (AC-CERT) **signed using the X.509 Federation Certificate** issued by the FA (SUB-CERT)
➔ **Include the chain <FA-CERT, SUB-CERT, AC-CERT> in the x5c parameter** of the JWK in the Metadata and use it during operational phase

Before Registration

→ **Generate Trusted Lists** including **X.509 Registrar Certificate** making them **publicly available through new federation endpoints**



3

→ Validate Entity Configuration (check that it is signed with private key related to the Federation public key)
→ **Generate X.509 Certificate** attesting Federation public keys and **signed with X.509 Registrar Certificate** (FA-CERT)
→ Generate Subordinate Statement **including X.509 Federation Certificate** (SUB-CERT) **in JWK Object (x5c parameter)**

4

→ **Update Trusted Lists** with SUB-CERT

Entity Configuration (Leaf)

Signed by SUB-CERT

```
{
"sub": "https://rp.example.it",
"iss": "https://rp.example.it",
"authority_hints": [
 "https://fa.example.it",
 ...
],
"jwks": {
 "keys": [{
   ...
  "x5c": [ <FA-CERT>,< SUB-CERT> ]
 }]
},
"metadata": {
 "openid_credential_verifier": {
  ...
  "jwks": {
   "keys": [{
     ...
    "x5c": [ <FA-CERT>, <SUB-CERT>, <AC-CERT> ]
   }]
  }
 }
},
...
}
```

Included in EC

Signed by

Signed by

Subordinate Statement

Signed by FA-CERT

```
{
"sub": "https://rp.example.it",
"iss": "https://fa.example.it",
"jwks": {
 "keys": [{
   ...
   "x5c": [ <FA-CERT>, <SUB-CERT> ]
 }]
},
"metadata_policy": {
   ...
},
...
}
```

Published in TL

Used for authentication to the Wallet Instance

Trusted List

Signed by FA-CERT

```
<?xml version="1.0" encoding="UTF-8"?>
<TrustServiceStatusList xmlns=<"...">
SchemeOperatorName="...">
  <SchemeInformation> ... </SchemeInformation>
  <TrustServiceProviderList>
    <TrustServiceProvider>
      <TSPInformation> ... </TSPInformation>
      <TSPServices>
        <TSPService>
          <ServiceInformation>
            <ServiceTypeIdentifier> ... </ServiceTypeIdentifier>
            <ServiceName>
              <Name xml:lang="en"> ... </Name>
            </ServiceName>
            <ServiceStatus>granted</ServiceStatus>
            <StatusStartingTime> ... </StatusStartingTime>
            <ServiceDigitalIdentity>
              <DigitalId>
                <X509Certificate> <FA-CERT> </X509Certificate>
              </DigitalId>
            </ServiceDigitalIdentity>
          </ServiceInformation>
        </TSPService>
      </TSPServices>
    </TrustServiceProvider>
  </TrustServiceProviderList>
</TrustServiceStatusList>
```

Interoperability:

- Keys in X.509 Certificate format included in JWK claim
- Federation APIs extended with Trusted Lists Endpoints

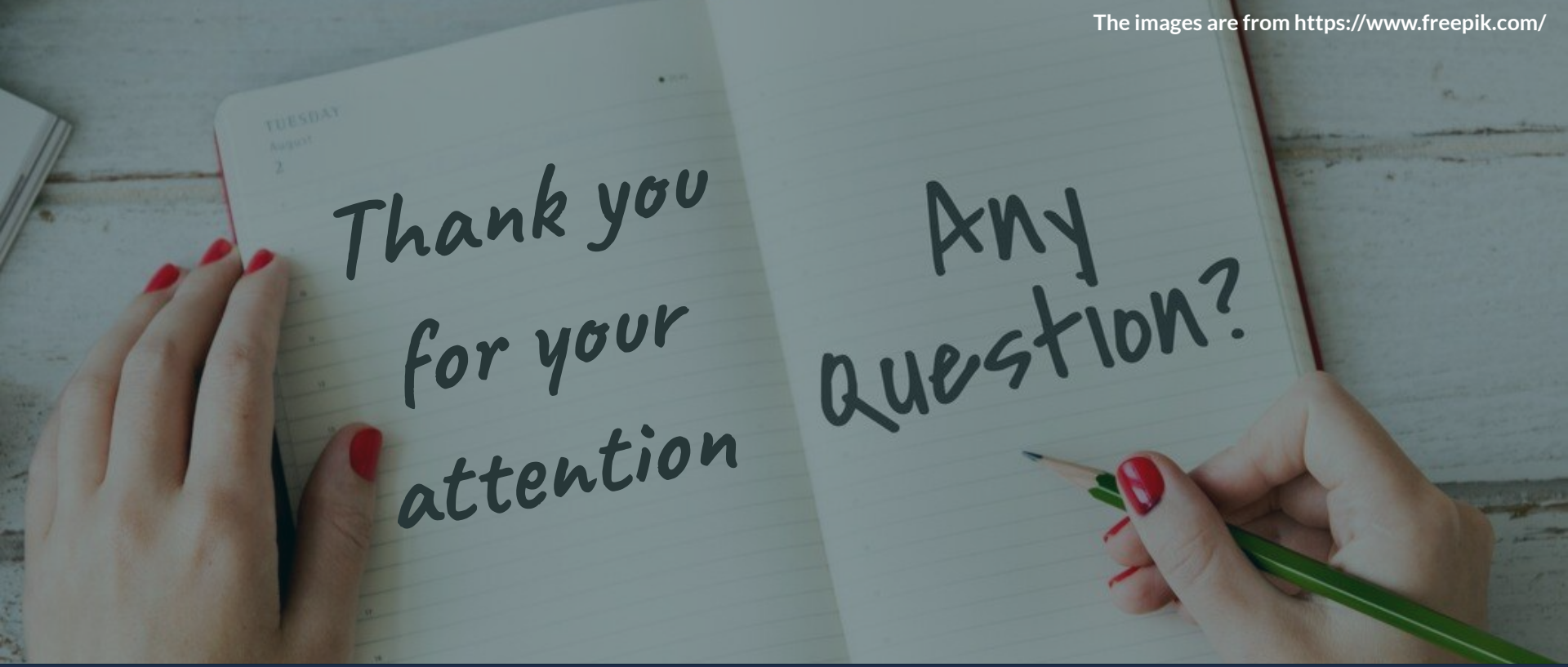
Scalability: Automatic and flexible Certificate update using OpenID Federation features

Integration with National Trust Frameworks: OpenID Federation and EU Trusted Lists can co-exist without breaking interoperability

Possible Alternative:

"**Automatic Certificate Management Environment (ACME) with OpenID Federation 1.0**"

→ it allows Federation Authorities in the OpenID Federation context to issue X.509 certificates attesting keys included in an Entity Configuration (currently under analysis)



The images are from https://www.freepik.com/

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

Pasquale Cerqua <p.cerqua at ipzs.it>

Francesco Antonio Marino <fa.marino at ipzs.it>